ABSTRACT

A method of deterministically generating maximal nonlinear block substitution tables for a predetermined block size is disclosed. The method includes selecting a first generating function and selecting a second generating function. The method also includes selecting first and second sets of complete linearly independent numbers, and calculating first and second linear orthomorphisms from the generating functions and the sets of linearly independent numbers. The method further includes creating maximal nonlinear block substitution tables by combining the linear orthomorphisms. The block substitution tables are for use in encrypting clear text messages.